

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW MEXICO**

UNITED STATES OF AMERICA,

Plaintiff,

vs.

CR. No. 16-4571 JCH

GUY ROSENSCHEIN,

Defendant.

MEMORANDUM OPINION AND ORDER

This matter is before the Court on *Defendant Dr. Rosenschein’s Motion for the Court to Order the United States to Disclose Expert Reports and the Bases and Reasons for Those Expert Opinions . . .* [Doc. 212]. After reviewing the motion, the Government’s response, the Defendant’s reply, the Government’s surreply, and the amicus brief filed by Microsoft, the Court concludes that the motion should be denied.

BACKGROUND

In July and August of 2016, the Bernalillo County Sheriff’s Office (“BCSO”) received two CyberTipline Reports from the National Center for Missing and Exploited Children (“NCMEC”). The two CyberTipline Reports were generated by Chatstep, an electronic service provider that hosts internet-based conversation (also known as “chats”) between users. In those CyberTipline Reports, Chatstep notified NCMEC that images of child pornography were uploaded through its service by a user identified as “Carlo.”

Chatstep was able to identify the images by using PhotoDNA. PhotoDNA is a computer program or software developed by Microsoft and available for organizations to use in order to help

prevent the sharing of harmful, child exploitation images. PhotoDNA works by obtaining the hash value of a file and converting the file into a numerical value that is matched against databases of hash values of known child pornography. Through its use of PhotoDNA, Chatstep identified the two images distributed by “Carlo” as child pornography before the images were submitted to NCMEC. NCMEC then forwarded the material to the New Mexico Attorney General’s Office Internet Crimes Against Children (“ICAC”) Task Force, and BCSO initiated a criminal investigation. After further investigation, BCSO obtained a state search warrant for Defendant’s residence. During the execution of the state search warrant on November 8, 2016, law enforcement located a thumb drive attached to a keychain found in the ignition of Defendant’s vehicle, which was found to contain images and videos of child pornography.

DISCUSSION

I. The Witnesses at Issue

The witnesses in question are John Shehan, Vice President of the Exploited Children Division of the National Center for Missing and Exploited Children (“NCMEC”), and Jeff Lilleskare, Group Manager for Security and Online Safety at Microsoft. Each of them has provided Defendant and the Court with two affidavits in connection with previous motions in the case.

Shehan, who has worked for NCMEC since February 2000, is responsible for supervising NCMEC’s CyberTipline and is familiar with its origins and operations, including the receipt and processing of reports by NCMEC and the procedures used to generate and maintain reports. Doc. 72-1. He also can explain the content of a CyberTipline Report. Id. In his supplemental declaration, Shehan discusses creation of the CyberTipline and some of the options available to users who submit a report to NCMEC. Doc. 94-2. He also describes the ways in which NCMEC uses CyberTipline Reports, the nature of feedback that NCMEC receives from law enforcement, and a

description of how NCMEC shares hash values with electronic service providers. Id. However, nothing in either of his affidavits indicates that Shehan is a software engineer, that he is familiar with the design and function of PhotoDNA's underlying computer code, or that he either intends or is qualified to testify on that subject.

Lilleskare's affidavit states that he is familiar with Microsoft's PhotoDNA technology. Doc. 82-6. He asserts that Microsoft acknowledges a responsibility to provide its customers with tools for online safety and discusses various Microsoft products that include "family safety technology tools," as well as the company's Digital Crimes Unit. Id. He asserts that PhotoDNA reflects Microsoft's "voluntary business strategy to protect its customers, systems, and reputation by creating a safer online environment." Id. He provides a general description of the concept of hashing and PhotoDNA, as well as the fact that Microsoft makes PhotoDNA available to certain application developers like Chatstep. He explains the systems by which developers can report images to Microsoft for hashing and comparison, as well as another system for enabling developers to create a Cybertip reporting hash matches to NCMEC by routing it via Microsoft. Id. *See also* Doc. 94-1. Like Shehan, nothing in Lilleskare's affidavits suggests that he will testify to anything requiring familiarity with PhotoDNA's algorithms and associated software.

II. The Arguments of the Parties

Defendant argues that prior to the upcoming evidentiary hearing on his motions to suppress, the Court should order the Government to produce expert reports for Shehan and Lilleskare. Defendant advocates for the disclosure of the opinions of these witnesses, as well as the bases and reasons for those opinions, and contends that if the Government declines to produce them, it should be prohibited from introducing the witnesses' testimony at the hearing.

Defendant's argument is two-pronged. First, he contends that Shehan and Lilleskare have specialized knowledge as defined by Rule 702 of the Federal Rules of Evidence. Second, he argues that he is entitled to their expert reports in advance of the hearing under Rule 16(a)(1)(G) of the Federal Rules of Civil Procedure. Rule 16(a)(1)(G) provides, in pertinent part: "At the defendant's request, the government must give to the defendant a written summary of any testimony that the government intends to use under Rules 702, 703, or 705 of the Federal Rules of Evidence during its case-in-chief at trial." Thus, by its express terms, Rule 16(a)(1)(G) does not apply to pretrial hearings, but only to the Government's case-in-chief at trial. Further, it is widely accepted that, apart from questions of privilege, the Federal Rules of Evidence do not apply in suppression hearings. *See United States v. Matlock*, 415 U.S. 164, 172-74 (1974). *See also* Fed. R. Evid. 104(a) (stating the court is not bound by rules of evidence when deciding preliminary matters concerning the admissibility of evidence); Fed. R. Evid. 1101(d)(1) (stating evidence rules are inapplicable to "[t]he determination of questions of fact preliminary to admissibility of evidence when the issue is to be determined by the court under rule 104.").

In response [Doc. 220], the Government makes a threefold argument: first, Rule 16(a)(1)(G) does not apply to suppression hearings; second, Lilleskare and Shehan are not expert witnesses; and third, the Government has already disclosed more information about their testimony than Rule 16(a)(1)(G) requires. With regard to the latter, the Government points to the two affidavits that each witness has already provided to the defense.

In his reply brief [Doc. 231], Defendant alters and expands his discovery request. He now asks the Court to order the Government to produce "expert reports, *in addition to the computer software or programs . . .* that their expert witnesses intend to testify about." Doc. 231 at 1 (emphasis added). Defendant's motion and supporting brief did not ask for the underlying

PhotoDNA computer code and related software. However, in the reply Defendant argues that because both Shehan and Lilleskare will testify about PhotoDNA, the reasons it was developed, and the ways in which it is used, he is “entitled to the raw materials about which these two individuals will testify in order to effectively cross examine them.” Doc. 231 at 2. He acknowledges that neither witness has any first-hand knowledge about what the computer programs contain or do, but rather they will testify about the results the programs generate. Nevertheless, Defendant maintains that he needs the computer code to test the veracity of their testimony and that without it he cannot conduct meaningful cross examination.

Defendant’s reply prompted both an amicus reply brief [Doc. 256] by Microsoft and a surreply brief [Doc. 245] from the Government. In its surreply, the Government notes that in his reply Defendant had broadened the scope of his request and argues that he had mischaracterized the expected testimony from Shehan and Lilleskare. It contends that they will testify to the “business and service operations of their respective companies,” and that Lilleskare has only a “working knowledge” of PhotoDNA functions, not “technical expertise” as to its inner workings. Doc. 245 at 2. The Government points out that this Court has already denied prior attempts by Defendant to obtain the PhotoDNA source code. And finally, it argues that the computer code is not material to the defense.

In its amicus brief, Microsoft argues that by asking the Court to compel the Government to produce the PhotoDNA algorithm and related software, Defendant is in fact asking the Court to compel Microsoft to produce it, since it is proprietary information not in the Government’s possession. Microsoft contends that request violates the discovery agreement it reached with Defendant in which Microsoft agreed to produce certain information to Defendant in exchange for his agreement to refrain from serving any new Rule 17(c) subpoenas on Microsoft, including a

subpoena pertaining to the PhotoDNA algorithm. It attaches email correspondence between counsel for Defendant and counsel for Microsoft documenting this agreement. Microsoft further argues that the requested computer code is irrelevant to the testimony that Lilleskare will offer at the suppression hearing, which includes how PhotoDNA was developed and how it functions but does not include information about the inner workings of the algorithm.

III. Analysis

Defendant acknowledges that neither Rule 16(a)(1)(G) nor the Rules of Evidence apply in a pretrial evidentiary hearing such as a hearing on a motion to suppress. But he asks the Court to disregard this accepted authority by arguing that “in other federal suppression hearings the United States has secured orders compelling defense experts to produce such reports and their underlying bases.” Doc. 212 at 11. As evidence of this, he points to a single unpublished slip opinion in *United States v. Ruiz*, Case No. 3:10-CR-254, Doc. 75 (M.D. Tenn. Mar. 16, 2011). *See* Doc. 212-2. In *Ruiz*, the Government successfully persuaded the district court to compel the defendants to disclose the identities and expert reports of their expert witnesses in advance of the suppression hearing, arguing that such a ruling would be supported by Rule 16(a)(1)(G). Anticipating (correctly) that the Government would argue that Rule 16(a)(1)(G) does not apply in suppression hearings, in this case Defendant now argues that the Government should be bound by the legal argument it made nine years ago in the *Ruiz* case. In that vein, he cites *Dugan v. EMS Helicopters*, in which the court stated that “inconsistent allegations contained in prior pleadings are admissible in subsequent litigation.” *Dugan v. EMS Helicopters, Inc.*, 915 F.2d 1428, 1431 (10th Cir. 1990). In *Dugan*, the plaintiffs alleged that a helicopter crash was proximately caused by the negligence of the helicopter manufacturers and helicopter maintenance company. The Tenth Circuit concluded that these allegations were factually inconsistent with the position that plaintiffs took in a subsequent lawsuit

arising from the same crash against the helicopter owner and operator and were admissible in evidence as “admission against interest.” *Id.* at 1431-32. However, the situation in *Dugan* is nothing like the one here. *Dugan* was a civil case in which the same plaintiff took different positions as to the cause of a single accident. *Dugan* does not support binding the Government to a legal argument that made nine years earlier in an unrelated criminal case prosecuted by different counsel in a different court.

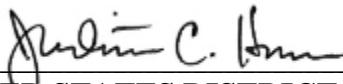
The Court is unpersuaded by Defendant’s argument and declines to apply Rule 16(a)(1)(G) in the manner suggested by Defendant. As a result, the motion will be denied. The Court’s primary reason for denying the motion is that the request is outside the scope of Rule 16(a)(1)(G). By its express terms, that Rule simply does not apply to this pretrial evidentiary hearing, but only to the Government’s case-in-chief at trial. It may be true that in certain circumstances the Court has the discretion to order expert reports in advance of a suppression hearing, but that does not mean that it necessarily should. Such an order would be outside the norm, and therefore this Court would require a significant showing be made that principles of fairness and justice require it. As further explained below, that showing has not been met here.

The secondary reason for the Court’s ruling is that requested expert reports are unnecessary. Even if Shehan and Lilleskare are expert witnesses—an assumption that the Court will make for the sake of argument, but which it does not reach—the declarations already filed by the Government adequately disclose the witnesses’ qualifications, opinions, and bases for those opinions and thereby satisfy the requirements of Rule 16(d)(1)(G). The testimony that Shehan and Lilleskare will offer at the hearing is not shrouded in mystery. In fact, Shehan has testified in similar cases to this one, and Defendant has apparently availed himself of that testimony, having cited it to the Court in various briefs in this case. *See, e.g.*, Doc. 231 at 13; Doc. 222 at 3. With

regard to PhotoDNA, Defendant has failed to demonstrate how disclosure of the underlying computer code will aid him in cross examining either Shehan or Lilleskare, neither of whom claims to have any knowledge or understanding of the code. He has also failed to explain how access to the computer code will help in proving the theory at the heart of his motions to suppress—that in developing PhotoDNA, Microsoft has acted as a government agent.

Third, Defendant's request for the PhotoDNA program is further undermined by two related facts: the Court already denied Defendant's request for this material, *see* Doc. 199 at 11-12 (listing categories of documents that Microsoft must produce that does not include computer code), and Defendant explicitly agreed not to seek the computer code from Microsoft in exchange for Microsoft's production of certain other materials. The fact that Defendant now seeks to obtain the PhotoDNA program from the Government instead of from Microsoft is a distinction without a difference. The Government would have to obtain the PhotoDNA computer code from Microsoft, and the Government would merely be a conduit.

IT IS THEREFORE ORDERED that *Defendant Dr. Rosenschein's Motion for the Court to Order the United States to Disclose Expert Reports and the Bases and Reasons for Those Expert Opinions . . .* [Doc. 212] is **DENIED**.



UNITED STATES DISTRICT JUDGE